Information Security Management

UNIVERSITY OF LEEDS

Use of Computer Systems Policy (Incorporating Internet, Web & Email Acceptable Usage)

Version 4-1-0

1st March 2017

Owner:	Kevin Darley, IT Security Co-ordinator, Information Systems Services, University of Leeds
Source Location:	
Document Reference:	
Other Documents Referenced:	
Related Documents:	Information Security Policy Password Usage & Management Policy Systems Security & Network Access & Management Policy Mobile & Remote Working Policy Software Usage & Control Policy Archiving Policy
Acknowledgements:	

Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes
1.0	28/05/04	http://campus.leeds.ac.uk/isms	First formal issue
2.0	09/07/04	http://campus.leeds.ac.uk/isms	Changes to 3.3 at the request of the AUT
2.1	19/08/04	http://campus.leeds.ac.uk/isms	Addition of copyright statement to front cover.
2.2	15/12/04	ISG	Amendments to 3.3, 3.8, 3.9 & Appendix A. New Sections 3.9.1, 3.9.2, 3.9.3 & Appendix B.
2.3	13/07/05	http://campus.leeds.ac.uk/isms	Addition of text to 2.2
2.4.	19/07/05	http://campus.leeds.ac.uk/isms	Amendment to 3.8 (deletion of text and x-ref to Access Control & Account Management Policy) & 3.9.1 (Addition of authorisation suffix text).

2.5	24/03/06	http://campus.leeds.ac.uk/isms	Various changes throughout
2.6	25/05/07	http://campus.leeds.ac.uk/isms	Inclusion of BCC field usage at 10.3.3 and removal of Maureen Harrison from Appendix A.
2.7	22/08/07	http://campus.leeds.ac.uk/isms	Section 3.3 - Additional rules concerning the posting of offensive material on Facebook & YouTube
2.8	30/08/13	http://iss.leeds.ac.uk/info/357/isms/	Amendment to process at Annex B
3.0.	20/04/15	http://it.leeds.ac.uk/info/116/policies	Addition of monitoring rights to 3.7, update from ISS to IT, update of cross-references and further minor amendment following feedback from ISG on 19/03/15.
4-0-0	07/03/16	http://it.leeds.ac.uk/info/116/policies	Cosmetic changes throughout and addition to 3.3 to address Prevent requirements
4-1-0	01/03/17	http://it.leeds.ac.uk/info/116/policies	Added clarity under 2.3 regarding software licensed for academic purposes

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://it.leeds.ac.uk/info/113/policies_and_information_security. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

Contents

1. Introduction

1.1. Background

University data must be protected against unauthorised access to and modification of its data and those using university information systems must do so within the framework of the law and other regulations.

The technical controls that are used within the University provide an essential element of the required protection. However, these only deliver part of the solution, the most effective defence being achieved through awareness and good working practices.

This document which forms the University's Use of Computer Systems Policy (incorporating Internet, web and email usage) in support of the University's Information Security Policy, defines both acceptable and unacceptable usage of IT/IS facilities, contributing to the overall goal of systems and information management. The University's full list of Supporting Policies within the Information Security Management System (ISMS) framework can be found at http://it.leeds.ac.uk/info/113/policies_and_information_security.

1.2. Applicability

This Policy concerns:

- The use of University owned IT and IS assets; and,
- University network facilities (wired and wireless) regardless of whether these are used through the connection of University assets or through the connection of private equipment (where this has been authorised).

It applies to the following:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of the University;
- staff who are employed by the NHS who are located at the University;
- students studying at the University;
- contractors and consultants working for or on behalf of the University;
- all other individuals and groups who have been granted access to the University's IT/IS and network facilities, including visitors.

It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, Deans and Heads of Schools/Services* are responsible for implementing this Policy within their respective faculty/department and for overseeing compliance by staff under their direction or supervision.

1.3. Scope

This Policy concerns all computer systems and network facilities operated by the University, regardless of location, where responsibility for user management and control resides with members of the University, or is outsourced to third parties.

* Also generically infers Heads of Centres & Institutes throughout.

2. Use of University Computer Systems

2.1. Conditions of Use

You may use the University's IT/IS and networking facilities if you have been authorised and are:

- An employee of the University;
- a student registered for any course at the University;
- a retired (as distinct from resigned) member of staff;
- an individual or a member of a group who has been permitted such access by someone with the appropriate authority;
- a visitor to the University.

Anyone else wishing to use a University computer system, or wishing to connect equipment to the University's network, must contact the appropriate faculty or department User Representative for the system concerned, or in the case of or for those requiring access to IT systems, the IT Service Desk.

As soon as a user/group ceases to satisfy any of the above criteria, they lose the right to use all University IT/IS and network facilities.

The University's IT/IS infrastructure and networking facilities may only be used with the correct authorisation. Only system administration staff for the respective computer systems can give that permission and may refuse it if it is reasonable to do so.

A username entitles an individual user *or* group of users to use computer systems for their own University or personal work only. The majority of services are free of charge at the point of use. However, certain specialist facilities, such as printing, may be charged for.

Users must not try to use anyone else's username and password which must be used and managed in accordance with the Password Usage & Management Policy. Users must not let anyone use their username and password, which must remain secret, except where this required to be divulged and used as part of a formal investigation, in accordance with the Security Incident & Computer Misuse Policy.

Where usernames lapse on a timed basis, the individual or group name becomes invalid and will no longer provide access to systems. However, files associated with the user/group will be retained for a reasonable period of time and can be retrieved if necessary. A lapsed username will be re-instated on request where such applications are supported by the correct authority.

2.2. Use of Private Equipment

Privately owned equipment belonging to staff (including post-graduates) is not to be connected to the University's wired network without authorisation from IT or the respective User-Representative. Only privately-owned equipment which is registered with IT and which is virus free and patched fully up to date will be granted authorisation for wired network connection.

Provision may need to be made for under-graduate students with special needs to connect their private equipment to the University's wired network. These issues are addressed through the Systems Security & Network Access & Management Policy.

A condition of wired network connectivity of privately owned equipment is that IT, and where applicable local computer support staff, reserve the right to apply service packs, fixes, work-a-rounds and patches, either physically or electronically to such equipment, and reserve the right to install anti-virus software and other software (in accordance with relevant licence conditions – see Software Usage & Control Policy) to allow remote security maintenance.

The University accepts no responsibility for the effects that any such installation may have on the operability of privately owned devices, consequently all risks, however small, reside with the owner.

Visitor's equipment may only be connected to the University network when the respective conditions of the Systems Security & Network Access & Management Policy and the Access Control & Account Management Policy have been met.

When connected to the University's networks, privately owned equipment may be monitored in accordance with Section 3.7. Any such equipment that is connected to the University network which is attributed to security problems or which causes security concerns may be disconnected without prior notification, and in certain circumstances, the user may be held accountable.

All equipment which is used to remotely connect to the University's network services and computer resources is governed by the Mobile & Remote Working Policy and the Systems Security & Network Access & Management Policy.

2.3. Laws, Regulation and Proper Practices

All use of University IT and IS facilities, including all University networks, must be in full compliance with English law, and where appropriate, all other regulations which are applicable.

You must not try to gain unauthorized access to any computer system anywhere. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990. In certain cases, such activities can also be contrary to other legislation, for example, The Terrorism Act 2000.

You must abide by any JANET Acceptable Use Policy and University Policies, Standards and Codes of Practice relevant to the use of computers, software and networks that are in place at any time, including those specific to faculties/departments, as applicable.

You must not do anything maliciously, negligently or recklessly which might cause any sort of harm or disruption to any computer system anywhere (worldwide), or to any of the programs or data on any system. In this context the word harm is taken to mean any kind of damage, and any kind of unauthorised access, denial of resources or any data alteration.

If you are reasonably requested to do so, you must justify your use of University IT/IS and/or networking facilities. You must explain (in confidence, if necessary) what you are doing, and how and why you are doing it. You must make any reasonable changes requested by IT staff or the departmental computer representative and comply with any reasonable restrictions placed upon you.

You must comply with valid regulations covering the use of software and datasets, whether those regulations are made by law, by the producer or supplier of the software or datasets, by the University or IT, or by any other legitimate authority. Software that is licensed for academic purposes only must not be used for commercial purposes, unless you have explicit permission to do otherwise[DN1]. Where you have any doubts you must contact IT or your faculty/departmental computer representative, as applicable, before using the software or dataset.

Unless you have proper permission from the appropriate person or organisation, you must not copy software (even as a backup copy) or share it or make it available in any way to anyone else. Failure to comply with this requirement could constitute a criminal offence under The Copyright, Designs and Patents Act 1988 and The Copyright, etc. & Trade Marks (Offences and Enforcement) Act 2002. All software is to be used, managed and controlled in accordance with the Software Usage & Control Policy.

The Data Protection Act 1998 regulates the use and storage of personal information (i.e. any information which identifies a living individual) on computing systems. It is your responsibility to ensure that your information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both you and the University. The University's Code of Practice on Data Protection can be found here.

2.4. Liability, Warranty and Related Matters

Whilst every reasonable endeavour is made to ensure that the IT/IS and networking facilities are available as scheduled and function correctly, no liability whatsoever can be accepted by the University for any direct or consequential losses or delays as a result of any system malfunction.

Whilst every reasonable endeavour is made to ensure the integrity of software products, the University does not offer any warranty on any software or its support. Accordingly, no liability can be accepted in consequence of any such product producing incorrect results or failing to work as documented. Responsibility for ensuring that software is suitable for the purpose for which it is used, or that any result obtained through IT/IS or network facilities is correct, always rest with the respective individual.

Whilst every reasonable endeavour is made to ensure the integrity and security of information held on computer media, no consequent liability can be accepted as a result of any such information being inadvertently lost, corrupted or inappropriately accessed. This includes programmes and data held on privately owned equipment when connected to the University's networks in accordance with 2.2.

Whilst every reasonable endeavour is made to ensure the accuracy of advice and information provided by the University, no liability can be accepted by the University for any consequential damages or losses arising from its use.

3. Internet, WEB and Email Usage

3.1. Policy Requirements

Those who use email or who create, manage or use web sites are responsible for ensuring that their usage complies with the legislative requirements outlined below. Those who manage such facilities are governed by the Systems Security, Network Access & Management Policy which details applicable legislation and technical control requirements.

3.2. Connectivity

Users will be provided with Internet, web access and email facilities either by Local Area Network (LAN) connectivity, Wireless LAN connectivity, via Virtual Private Network (VPN) or through Thin Client Technology connections. In addition, some University computing resources are available through web services.

Access to these facilities is granted subject to compliance with the legal requirements, behavioural standards and responsibilities specified within this Policy. Additional requirements for 'mobile and remote access' (including home working) are defined in the Mobile & Remote Working Policy.

3.3. Conditions Applicable to All Users[1]

University IT/IS facilities must not generally be used for, or in connection with, the following activities (I. to XV) some of which could result in legal action or civil proceedings being mounted against either an individual, the University, or both.

I. Deliberately accessing, creating or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, with the exception of data which is connected with University work or official research or other professional activity, where the sender/recipient would expect to exchange such material with other users in a professional capacity;

II. Creating, transmitting or accessing material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another, with the exception of data and email traffic which is connected with University work or official research or other professional activity, where the sender/recipient would expect to access, or exchange such material with other users, in a professional capacity;

III. Creating, transmitting or accessing material which runs the risk of drawing people in to, or towards, terrorism, except where it can be demonstrated that there is a legitimate academic interest[2];

IV. deliberately contributing to News Groups or web sites that advocate illegal activity;

V. creating or transmitting defamatory material or material that is libellous of any other person's or company's reputation, products or services;

[1] Individuals must be able to justify for purposes of official research any contravention Conditions. Anyone who wishes to carry out research activities contrary to these Conditions must notify the IT Service Desk of their intentions before using University IT and IS systems for those purposes.

[2] Those that do have a legitimate academic interest in this material might choose to register their interest with the University Secretary in advance (via the IT Security Team at cybersecurity@leeds.ac.uk)

VI. viewing, transmitting, copying, downloading or producing material, including (but not exhaustively) software, films, television programmes, music, electronic documents and books which infringes the copyright of another person, or organisation;

VII. making offensive or derogatory remarks about staff, students or the University on interactive social and life-style websites such as Facebook;

VIII. posting offensive, obscene or derogatory photographs, images, commentary or soundtracks on interactive social and life-style websites such as Facebook and YouTube;

IX. transmitting or producing material which breaches confidentiality undertakings;

X. attempting to gain deliberate access to facilities or services which you are unauthorised to access;

XI. deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste staff effort or networked resources;

XII. creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe;

XIII. making commitments via email or the Internet on behalf of the University without full authority;

XIV. undertaking any activities detrimental to the reputation or business interests of the University;

XV. initiating or participating in the sending of chain letters, 'junk mail', 'spamming' or other similar mailings.

Any user who inadvertently accesses an inappropriate Internet site must immediately close the session or return to the previous page.

Any member of staff who receives an inappropriate email message or email content that appears to have been sent by a member of staff or student may wish to report the matter to their line manager. Students may report any such occurrences to either their tutor or to IT Service Desk staff.

3.4. Other Restrictions Applicable to Staff and Students

Staff and students must obtain formal University permission before using University computer resources[3] for any work which is funded (partly or wholly) by any person or organisation outside the University or on any consultancy basis.

Permission for such work to be undertaken on University systems may be refused, but where it is granted, a charge may be applicable.

Students must obtain formal University permission before using University computer resources[*] for any work which is in connection with any person or organisation outside the University, regardless of whether it is funded or not. They may be given a separate username which must be used for all associated computing activity and charges may be incurred.

[3] All references to computer or network resources include network connections (physical and wireless), routing and switching.

3.5. Additional Restrictions Applicable to Students in Residences

The following additional restrictions apply to students in residences who access University network resources*, regardless of whether network connection is effected using privately owned equipment, through equipment owned by the University, or via equipment owned by any third party.

Each student is responsible for maintaining effective security of their equipment attached to the University network, by updating service packs, applying security patches and maintaining up to date virus protection software etc.

The resale (or making available to others without charge) of network and computing services (for example through hubs, proxy services or wireless facilities) is prohibited.

Privately owned and third party equipment connected to the University network may be subjected to the same monitoring activities as the University's own equipment (Ref. 3.7). Logs of computer system usage may be taken and may be scrutinised. These will be retained for periods appropriate for operational purposes.

The University accepts no responsibility for the security of any privately owned or third party owned computer attached to its network, or any liability for any damage to any such device how so ever caused. This disclaimer also extends to any other network which the University does not provide (including its components) to which private, third party or University equipment may be attached by a student.

The University reserves the right to restrict or block any device or services which have an adverse affect on the University's network or which are resulting in a degradation of its network services.

Further details are available in Policies and Rules for Halls of Residence.

3.6. Website Management

The creators of websites are personally accountable for ensuring that the contents comply with the requirements of this Policy and relevant legislation. As such, except where anonymous input is allowed (for example guest books), scripting which enables others to alter the content is not to be made available to anyone who is not subject to this Policy. Where anonymous input is allowed this must be policed at regular and frequent intervals by the owner of the site to remove any inappropriate content and to prevent further site access by anyone posting such material.

The University's guidelines, codes and 'Acceptable Use Policy applicable to Web Pages', which can be found at http://comms.leeds.ac.uk/web/website-regulations/ are to be strictly adhered to by those creating and managing websites.

3.7. Monitoring the Use of Facilities

Under The Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) the University reserves the rights to monitor users' activities to:

- record evidence of official transactions;
- ensure compliance with regulatory or self-regulatory guidelines (including this Policy);
- maintain effective operations of systems (e.g. preventing viruses);
- prevent or detecting criminal activity;
- prevent the unauthorised use of computer and telephone systems – i.e. ensuring that the users do not breach University policies.

Under this regulation there is a requirement for employers to inform staff about such monitoring. The publishing of this Policy is one means of fulfilling that obligation.

In accordance with the above regulation, the University reserves the right to deploy software and systems that monitor, block or record all Internet access. These systems are capable of recording (for each and every user) exactly how much Internet usage is being conducted for each World Wide Web site visit (the date and time visited and how long was spent on the site), each email message, and each file transfer into and out of our internal networks. This right is reserved at all times, although it is anticipated that instances of such monitoring will be minimal and proportional to operational needs.

Privately owned equipment connected to University networks in accordance with 2.2 may be subjected to the same monitoring activities as University equipment.

In certain investigatory circumstances it may be necessary for the University to access emails of its staff and students, including emails which have been deleted. In such circumstances access will be proportionate to the requirement for the access and subject to privacy assessment.

Access to users' emails will be undertaken under strict conditions and only on the authority of either the Secretary to the University, the Deputy Secretary to the University, the Director or Deputy Director of Human Resources or the University's Legal Advisor. An audit trail will be maintained of all such access.

Logs of computer system usage will be taken and may be scrutinised. These will be retained for periods appropriate for operational purposes.

Data may be archived and the University reserves the right to examine this in accordance with 3.9, and to delete it.

3.8. Personal Use of Internet and Email[4]

Significant bandwidth and disk space overheads are incurred through Internet and email traffic usage, and for email and attachment serving and storage. In view of this, the University's IS/IT facilities are provided for operational and research purposes only. However, non-excessive and reasonable personal use of these facilities by staff[5] may be permitted provided that such use does not interfere with the work performance of the employee or the activities of other staff or students, and is wholly compliant with legislative requirements and the terms of this Policy.

Those who use University computing resources to make purchases, pay bills or conduct on-line banking or similar activities do so at their own risk. The University cannot be responsible for any direct or indirect losses sustained by those using its computer resources for personal transactions.

3.9. Privacy and Third Party Access

A degree of privacy can be expected in the private use of the University's computing facilities. However, all users should be aware that owing to the University's obligations (statutory and otherwise) there are limitations to the privacy that can be enjoyed.

[4] Director HR, and AUT, Amicus & Unison representatives previously consulted on this matter.
[5] What constitutes 'reasonable use' of resources for personal matters is at the discretion of the dean of each faculty or head of each school/service.

For operational purposes it may be necessary for the University to access email folders and file stores occasionally during periods of unexpected staff absence (or in accordance with 3.7 above). This applies when no-one else (such as personal assistants, secretaries etc., who are granted shared access to their manager's account on their manager's authority) can access the data required, and arrangements for them to do so could not have been made in advance of their absence.

Likewise, when staff have ceased University employment it may be necessary for IT staff to recover or copy archived data that needs to be subsequently accessed by faculty or department staff.

With these points in mind, you should not use University systems for the transmission or storage of any material that you would not wish others to see, and you should inform your correspondents not to send you material that is personal and which you or they wish to keep private.

Any University access to users' data in their absence, or when they have ceased University employment, is to be both controlled and accountable and must be in accordance with the requirements of the Access Control & Account Management Policy.

Any member of the University who is granted operational access to another user's data may only view material that it is considered necessary to see for the operational reason for which access was granted. They are required to treat all material as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted, and they must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters. A failure to do so could constitute an offence under the terms of the Human Rights Act 2000.

As an additional safeguard against inadvertent disclosure, staff may wish to precede the subject title with 'PRIVATE' in the subject line of any personal emails, or use the 'personal' or 'private' sensitivity settings available through 'message options' in Office 365 for Email.

It is stressed that any access to users' emails or data outside of the above controls could constitute a criminal offence.

3.10. Mass Mailing Restrictions and Controls

The University encourages and promotes the use of electronic mail to further its educational, research and service missions for legitimate academic and administrative pursuits. However, the sending of bulk University-wide / inter-faculty / departmental emails has to be regulated to prevent misuse or abuse. This Policy provides a framework for the authorisation of bulk, unsolicited emailing by any delivery means.

3.10.1 University-Wide and Inter-Faculty Emails

The distribution of University-wide emails by staff or students using the 'all staff address list' or 'all students address lists', or by harvesting global address lists is prohibited unless the messages have been formally approved by the University Secretary[6], or are sent by or on behalf of a member the University Executive Group. Messages that are sent outside of the authorisation process will not be released by the University mailing list moderators. The process for requesting authority to send bulk emails can be found at Appendix A.

Messages that are likely to be approved for University-wide distribution generally will be restricted to urgent operational matters that need to be brought to the attention of the University's members. However, this mechanism may also be used for notifying staff of certain personnel issues and for the undertaking of official University surveys.

[6] The University Secretary will delegate approval authority to other senior managers within the University.

Messages that may be approved as being appropriate for widespread distribution include, but are not limited to, those concerning:

- Security issues, such as bomb or terrorist threats and computer system viruses and other threats;
- health and safety matters such as hazard warnings and natural disaster alerts;
- urgent upgrades of the University's IT/IS services that may result in temporary disruption to systems;
- the announcement of University policies that are time critical or which members have to be made aware of for legal compliance reasons;
- informing students of new registration or examination information;
- informing staff of new pay structures or industrial action;
- important announcements from the University's executives/governance groups (Strategy Group, Senate, Council, etc.)
- time critical financial and administrative deadlines.

Anyone wishing to send an inter-faculty email must obtain authority for sending it from the dean of the faculty that will receive it.

All approved bulk email messages are to contain the following information:

- Subject line: with clearly stated subject:
- From: line that contains the email address of sender;
- To: line that includes University group/s to which the mass email will be sent;
- signature information providing the name, department and telephone number of the sender.

The email body is to contain:

- plain text only - graphics, bolding or other font styles are not permitted;
- no attachments - a link to an appropriate web page which includes the detailed information is to be provided by the sender;
- brief and to the point messages only, although instructions on how additional information can be obtained may be included.

Departments wishing to announce campus sponsored events should use the facilities available within the Student Portal or the 'for staff' website.

Alternatively, there is provision for users to subscribe to opt-in mailing lists.

3.10.2 Mass Mailing within Faculty

The dean of each faculty is authorised to send bulk emails to those members of their own faculty using the respective 'all staff lists' and respective 'all student lists', and may provide authority for other members of their faculty to do the same.

However, the use of faculty-wide mailing must be restricted to important matters where this communication mechanism is considered to be both appropriate and necessary to reach the required audience. Details of less important matters such as conferences, events, etc. are to be published using other facilities.

Those wishing to send a faculty-wide bulk email are to follow the process at Appendix B.

3.10.3 Mass Mailing – Mailing Lists, Address Book & Database Held Addressees

Users who send emails to multiple recipients by compiling a list from a personal address book or database are to enter the email addresses in the BCC field so that they cannot be seen and harvested by others.

With the exception of emails to mailing lists to which users have chosen to subscribe, such mailings are also include the following statement in the body of their mail: "*This email has been sent to you because you are considered to be a likely interested party in the subject matter. If you no longer wish to receive email of this nature please reply and your address will be removed from the list*".

All removal requests are to be actioned by the recipient on receipt.

3.11. Computer Crime and Misuse

The University expects users to use IS/IT facilities, and in particular email and the Internet, responsibly at all times.

Suspected computer crime and misuse of University IS/IT facilities, including excessive personal use by staff, will be investigated in accordance with the University's Security Incident & Computer Misuse Policy.

Members of staff should check and agree conditions of personal usage of computers with their Line Manager or Head of School/Service if they are in any doubt.

3.12. Use of Computer Clusters

The use of computer cluster facilities is governed by the Acceptable Use of Clusters.

4. Appendices

4.1. A – University-Wide, Inter-Faculty and Inter-Departmental Email

1. Anybody wishing to send a bulk email should email their request to the University Secretary at j.r.gair@adm.leeds.ac.uk and copy it to a.l.laverton@adm.leeds.ac.uk. This will enable the request to be forwarded to an alternative approval authority, should the University Secretary be unavailable.
2. The subject header of the email is to contain the wording "Bulk Email Request:" followed by the title of the message, so that it is immediately identifiable by the Secretary, or his support staff for forwarding to an alternative approval authority, in his absence.
3. The request should provide a brief explanation why the email needs to be sent out, who has approved the sending within the faculty/department, to whom it needs to be addressed (i.e. staff, students or all) and when it needs to be sent out.
4. Once the message has been compiled in accordance with Section 3.10.1 the requestor should complete the 'To' field and send the message[7].
5. The University mailing list moderators will receive the mail and release it to the addressees providing the process has been followed and the authority for the sending of it included.

[7] Messages to all staff should be addressed to allstaff@lists.leeds.ac.uk. Details should obtained from the IT Service Desk where there is a requirement to send an email to all students.

4.2. B – Authorisation and Process for Mass Mailing within Faculty

1. Anybody wishing to send a bulk email within their faculty should email their request to their respective dean or his/her nominated deputy.
2. The request should provide a brief explanation why the email needs to be sent out, to whom it needs to be addressed (i.e. staff, students or both) and when it needs to be sent out.
3. Having obtained the required authority, the requestor should:
   - Compile the body of the email and precede it with "This is a bulk email which has been sent to staff/students <*delete as appropriate*> within the faculty of <*add details*> on the authority of the dean. The purpose of this e- mail is to raise awareness of <*add detail*>;
   - complete the 'Subject' field;
   - enter the respective email addresses in the 'BCC' field (to prevent replies to all);
   - send the mail.